UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/976,050	10/15/2001	Saori Nishimura	P 282732 T41A-01S0063-1	1678

909	7590	05/31/2005

PILLSBURY WINTHROP SHAW PITTMAN, LLP
P.O. BOX 10500
MCLEAN, VA 22102

EXAMINER
HO, THOMAS M

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 05/31/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/976,050	NISHIMURA, SAORI
	Examiner	Art Unit
	Thomas M. Ho	2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *15 October 2001*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *4/22/04, 5/21/04*.

4)☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____ .

DETAILED ACTION

1.   Claims 1-9 are pending.

Claim Rejections - 35 USC § 112

2.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 9 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The Examiner is unable to precisely determine what is claimed by claim 9. The Applicant for example recites "third output means for outputting data to be encoded to the first IC card". Is applicant claiming that data is stored to the first IC card, or rather that such information is designed to be read and then outputted to another location?

The Examiner is also unable to determine the meaning of "setting a key". In particular, claim 9 recites a "first setting means for setting second and third keys." Does setting a key mean that the key is generated? Does it mean that the key is stored? Does it mean that a key remains in anticipation of being stored? Does it mean that a storage means is created for it so that the key may be stored? Does it mean that a key merely exists? Does it mean changing the values of the keys? Does it mean arranging them in a particular order? Does it mean confining the size of the

keys to a particular boundary or size? Does it mean placing the keys in a particular address or section of memory or the general system? Any one of these may be a reasonable interpretation to Applicant's claim recitation.

It should however be noted that although other claims such as claim 2, recite the phrase "key setting instruction", the rest of the claims provided a sufficiently detailed context that interpretation of the meaning of this phrase is not rendered vague and indefinite.

For example, claim 2, recites "first key setting means for storing a second key"

Claim 2 later recites, "transmitting a key setting instruction to which the second key is added to the two IC cards through the communication means." which would imply that the setting is to be read as a storage type instruction for an established key.

Claim 9 however, recites no such structural limitations so as to sufficiently breathe life and meaning to the phrase "first setting means".

Claim limitations such as "associating a key", or "setting a key", "setting a piece of data", are indefinite without further limitations because they may possess any number of meanings in the context of cryptography and computer technology. It is uncertain what applicant is claiming without proper contextual wording.

Claim Rejections - 35 USC § 102

3.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4.   Claims 1,3 are rejected under 35 U.S.C. 102(e) as being anticipated by Mooney et al.

In reference to claim 1:

Mooney et al. (Column 11, lines 7-16) & (Column 11, lines 17-35) discloses an IC card terminal

unit comprising:

- Communication means for communicating data between two IC cards in one of which at

    least a key for encoding or decoding data is stored and in the other of which the key is not

    stored, where the communication means for communicating data between two IC cards is

    a PC and it's memory, and the smartcard with the key is the owner smart card, and the IC

    card where the key is not stored is the guest smart card. (Column 11, lines 7-16)

- Key takeout means for taking out the key in the former IC card through the

    communication means by transmitting a key takeout instruction to the former IC card in

    which the key is stored through the communication means, where the key takeout means

is the ability to read the key from the IC card and the key takeout instruction is a request

for a direct key transfer. (Column 11, lines 7-16)

- Encoding-key setting means for storing the key in the above latter IC card by transmitting

    an encoding-key setting instruction to which the key taken out of the former IC card by

    the key takeout means to the latter IC card in which the key is not stored through the

    communication means, where the key taken out of the former IC card (owner smartcard)

    is stored in the latter IC card where the instruction to store the key in the latter IC card

    (guest smart card) is a "copy" type instruction. (Column 11, lines 7-16)

The second section (Column 11, lines 17-35) discloses an additional more specific embodiment

which discloses the limitations of claim 1.

In reference to claim 3:

Mooney et al. (Column 11, lines 7-16) & (Column 11, lines 17-35) discloses an IC card

duplication method using a first IC card to be duplicated in which at least a key for encoding or

decoding data is stored, a duplicating second IC card, and

- A terminal unit for handling these first and second IC cards(where the terminal unit is the

    apparatus allowing the keys to be transferred from the first IC card to the second),

    comprising:

- A first step of transmitting a key takeout instruction from the terminal unit to the first IC

    card, where the key takeout means is the means for reading the key from the owner IC

card through the smartcard reader(when the owner selects a key from (Column 11, lines

7-16), and the instruction for transmitting a takeout instruction is a request to export to

the key. (Column 11, lines 18-20)

- A second step of receiving a key takeout instruction transmitted from the terminal unit

  and transmitting the key to the terminal unit in the first IC card, where the key is

  transmitted from the IC card to the terminal unit when the key is extracted and stored in

  the memory of the PC. (Column 11, lines 10-15)

- A third step of receiving a key transmitted from the first IC card and transmitting an

  encoding-key setting instruction to which the received key is added to the second IC card

  in the terminal unit, where they key setting instruction is storing the key transmitted

  encoded key onto the guest smart card (Column 11, lines 15-16), and where the key is

  encoded (Column 11, lines 20-25)

- A fourth step of receiving the encoding key setting instruction transmitted from the

  terminal unit and storing a key added to the encoding-key setting instruction, where the

  encoded key is received and then stored (Column 11, lines 30-36) & (Column 11, lines

  15-16).

Claim Rejections - 35 USC § 103

5.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6.   Claims 2, 4-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over US patent 6351813, Mooney et al. Claim 9, as best understood is rejected under 35 U.S.C. 103(a) as being unpatentable over US patent 6351813, Mooney et al.

The Applicant has frequently recited the issuance of an instruction to initiate a particular set of actions in the claim limitations. For clarity of the record, the Examiner notes that all computer actions are stipulated by computer operations, also commonly known in the art of computer science as "instructions".

In reference to claim 2:

Mooney et al. (Column 11, lines 1-35) discloses an IC card terminal unit comprising:

- Communication means for communicating data between two IC cards, where the communication means is the "remote key transfer method" which is comprised of a network. (Column 11, lines 25-30)

- First key setting means for storing a second key for encoding or decoding a first key in the two IC cards respectively by transmitting a key setting instruction to which the second key is added to the two IC cards through the communication means, where the encoding or decoding of the first key(the key within the smartcard) is performed with a

second key, the encryption key which is converted from an authentication question.
(Column 11, lines 20-25)

- Key generation means for generating the first key for encoding or decoding data in the former IC card by transmitting a key generation instruction to one of the two IC cards, where the key generation means is the ability of the owner to generate a key (Column 10, lines 62-67) which is used for encoding data between two parties. (Column 11, lines 35-40)

- Key takeout means for taking out the first key generated in the former IC card generating the first key by the key generation means through the communication means by transmitting a key takeout instruction to the former IC card through the communication means, where the key takeout means is the means for reading the key from the owner IC card through the smartcard reader, and the instruction for transmitting a takeout instruction is a request to export to the key. (Column 11, lines 1-35)

Mooney et al. fails to explicitly disclose:
Confirmation means for confirming whether setting of the second key by the first key setting means normally ends.

The Examiner takes official notice that confirmation means for confirming whether an operation of a digital system was successfully completely was well known at the time of invention.

For Example, computer systems that use access messages such as "access denied" or "access granted", or "general protection fault" or "operation successful" or "save completed" or "format completed" are all confirmation means to indicated whether a given operation on a computer was successfully completed.

It would have been obvious to one of ordinary skill in the art at the time of invention to include a confirmation means for confirming whether setting of the second key by the first key setting means normally ends in order to allow a user to know whether or not the operations he or she chose to perform completed successfully.

In reference to claim 4:

Mooney et al. (Column 11, lines 7-35) fails to explicitly disclose the IC card duplication method of claim 3, wherein the key for encoding or decoding the data stored in the first IC card is generated in the first IC card in accordance with the key generation instruction input from the terminal unit.

Mooney discloses that the key is generated in accordance with key generation instruction input from the terminal unit (where the generation instruction instructs the key to be transferred and causes the answer to a security question to be converted into an encoding key), but does not disclose where this key is generated. It can be however inferred that the key is generated either on the smartcard or the PC.

For the most part, the location of the generation of information, or the site of computation is

unimportant and obvious to those of ordinary skill in the art. It is evident from Mooney et al.

that both the smartcard and the terminal unit itself contains a memory for storage. It is well

known in the art that memory is used for the site of the processing of data. For Example, while

data is being processed, there must be some memory for the processed information to be stored.

Such processing may be done in any memory.

It would have been obvious to one of ordinary skill in the art at the time of invention to generate

the key for encoding and decoding in the first IC card in order to maintain greater security by

having the generated encoding key remain completely confined to the smartcard thereby making

the compromising of the key more difficult.

Claim 5 is rejected for the same reasons as claim 4.

In reference to claim 6:

Mooney et al. (Column 11, lines 7-35) discloses an IC card duplication method using a first IC

card to be duplicated in which at least a first key for encoding or decoding data is stored, a

duplicating second IC card, and a terminal unit for handling these first and second IC cards,

comprising:

- A first step of transmitting a key-setting instruction to which a second key for encoding

  or decoding the first key is added from the terminal unit to the first and second IC cards,

where the key setting instruction is the instruction which initializes the key transfer

option, and the second key is the key generated to encrypt the key that is to be

transferred. (Column 11, lines 7-35)

- A third step of transmitting a key takeout instruction from the terminal unit to the first IC

  card, where the key takeout instruction instructs the first IC card to have its key read.

  (Column 11, lines 10-15)

- A fourth step of receiving the key takeout instruction transmitted from the terminal unit,

  encoding the first key by the second key stored in the second step, and transmitting the

  encoded first key to the terminal unit, where the first key is the key from the smartcard,

  the second key is the key used to encrypt the first key, and the transmission passed

  through the PC terminal unit. (Column 11, lines 7-35)

- A fifth step of receiving the encoded first key transmitted from the first IC card and

  transmitting an encoding-key setting instruction to which the received encoded first key

  is added to the second IC card in the terminal unit, where the encrypted or encoded first

  key is transmitted from the first IC card to be stored in the second unit, which is the guest

  smart card (Column 11, lines 7-35)

- A sixth step of receiving the encoding-key setting instruction transmitted from the

  terminal unit, decoding the encoded first key added to the encoding-key setting

  instruction by the second key stored in the second step, and storing the decoded first key

  in the second IC card, where key first from the user smart card is decoded or decrypted

  with the second key and storing the decoded key into the user smart card. (Column 11,

  lines 15-16)

Mooney et al. fails to explicitly disclose a second step of receiving the key-setting instruction

transmitted from the terminal unit and storing the second key added to the key-setting instruction

in the first and second IC cards.

Mooney simply discloses that this second encryption key must be sent to the user of the second

card.

It is evident from Mooney et al, however, that a key may be easily store a key, whether it be an

encryption key or regular key.

It would have been obvious to one of ordinary skill in the art at the time of invention to store the

key for encoding and decoding in the first IC card in order to maintain greater security by having

the generated encoding key remain completely confined to the smartcard thereby making the

compromising of the key more difficult. (for example, the keys may now be confined to

password access) (Column 3, line 67 – Column 4, line 5)

Claims 7, 8 are rejected for the same reasons as claim 4.

Claim 9 is rejected for the same reasons as claim 6.

Conclusion

7.   The following art not relied upon is made of record:

"The smartcard copier's user's guide", telesystems 2001, discloses an apparatus which

allows a smartcard to be copied.

- US patent 6,009,174 discloses a key transfer method similar to applicant's.

- US patent 6230267 discloses a method of transporting data such as a key onto an IC card.

8.   Any inquiry concerning this communication from the examiner should be directed to

Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be

reached on M-F from 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor,

Gregory A. Morse can be reached on (571)272-3838.

The Examiner may also be reached through email through Thomas.Ho6@uspto.gov

Any inquiry of a general nature or relating to the status of this application or proceeding should

be directed to the receptionist whose telephone number is (571)272-2100.

| General Information/Receptionist | Telephone: 571-272-2100 | Fax: 703-872-9306 |
| Customer Service Representative | Telephone: 571-272-2100 | Fax: 703-872-9306 |

TMH

May 11th, 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100